We claim:

Sub a1 1. A validation protocol for determining whether an untrusted authentication chip is valid, or not, including the steps of:

generating a random number and encrypting it with an asymmetric encryption function using a first key;

passing the encrypted random number to an untrusted authentication chip;

decrypting the encrypted random number with an asymmetric decryption function using a secret key, in the untrusted authentication chip;

comparing the decrypted random number with the original random number, and in the event of a match considering the untrusted chip to be valid;

otherwise considering the untrusted chip to be invalid.

2. A validation protocol according to claim 1, where the random number is not secret, but where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

3. A validation protocol according to claim 1, where the first key is a public key.

4. A validation protocol according to claim 1, where the encryption is implemented in software.

5. A validation protocol according to claim 1, where the encryption is implemented in a second authentication chip.

6. A validation protocol according to claim 1, where the keys used for encryption and decryption are 2048 bits or larger.

7. A validation system for performing the method according to claim 1, where the system includes a random number generator, an asymmetric encryptor to encrypt generated random numbers and a first key for the encryptor, and an untrusted authentication chip; the untrusted chip includes an asymmetric decryption function to decrypt encrypted random numbers and a secret key for the decryption function; a comparison means are also provided to compare a decrypted random number with an original random number, and in the event of a match considering the untrusted chip to be valid; otherwise considering the untrusted chip to be invalid.

8. A validation system according to claim 7, where the random number generator, encryptor and comparison means are in an external system.

9. A validation system according to claim 8, where the external system is in a device in which are mounted, and the untrusted chip is in the consumable.

10. A validation system according to claim 7, where the random number generator and encryptor are in a second authentication chip, and the comparison means are in an external system which receives the random number and the encrypted version before passing only the encrypted version to the untrusted chip; the system also receives back the decrypted version from the untrusted chip and performs the comparison.

11. A validation system according to claim 10, where the system is in a device in which consumables are mounted, and the untrusted chip is in the consumable.

12. A validation system according to claim 7, where the random number is not secret, but the random number generator includes a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

13. A validation system according to claim 7, where the first key is a public key.

14. A validation system according to claim 7, where the encryption is implemented in software.

15. A validation system according to claim 7, where the encryption is implemented in a second authentication chip.

16. A validation system according to claim 7, where the keys used for encryption and decryption are 2048 bits or larger.